1. INFORMACIÓN GENERAL

PROCESO O ACTIVIDAD: Sistema de Gestión de Seguridad de la Información con base en el estándar ISO/IEC 27001:2013 en los 18 procesos de la Autoridad Nacional de Licencias Ambientales (ANLA)	**FECHA DE LA AUDITORÍA:** Desde el Martes 29 de Agosto de 2023 Hasta el Lunes 04 de Septiembre de 2023
AUDITOR LIDER: Ángel Roberto Prieto Puentes *Consultor en seguridad de la información, ciberseguridad, continuidad del negocio y gestión de calidad* *Lead and internal Audit ISO IRCA 27001:2013 y 27001:2022* *Lead and internal Audit ISO 9001 Exemplar Global* *Internal Audit ISO 14001, ISO 22301 SGS* *SCRUM Master (SMPC, SPOPC)* *Empresa: Ingeteknia.*	**EQUIPO AUDITOR:** Ángel Roberto Prieto Puentes
AUDITADO:	Líderes de los 18 procesos de la Autoridad Nacional de Licencias Ambientales (ANLA). (Ver detalle en el Plan de Auditoría)
OBJETIVO:	Evaluar la conformidad del Sistema de Gestión de Seguridad de la Información con base en el estándar ISO/IEC 27001:2013 y de la normatividad del sector en función de los objetivos estratégicos de la ANLA.
ALCANCE:	Evaluación y seguimiento de licencias, permisos y trámites ambientales. Se excluyen el siguiente controle del anexo A, ISO/IEC 27001:2013 Control A.14.2.7. Desarrollo externo
CRITERIOS:	Estándar ISO/IEC 27001:2013, especificaciones propias de la organización, del sector y de legislación y normatividad aplicable.

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	29	**Mes**	08	**Año**	2023	**Desde**	29 / 08 / 2023 DD / MM /AA	**Hasta**	04 / 09 / 2023 DD / MM /AA	**Día**	04	**Mes**	09	**Año**	2023

2. ACTIVIDADES DESARROLLADAS

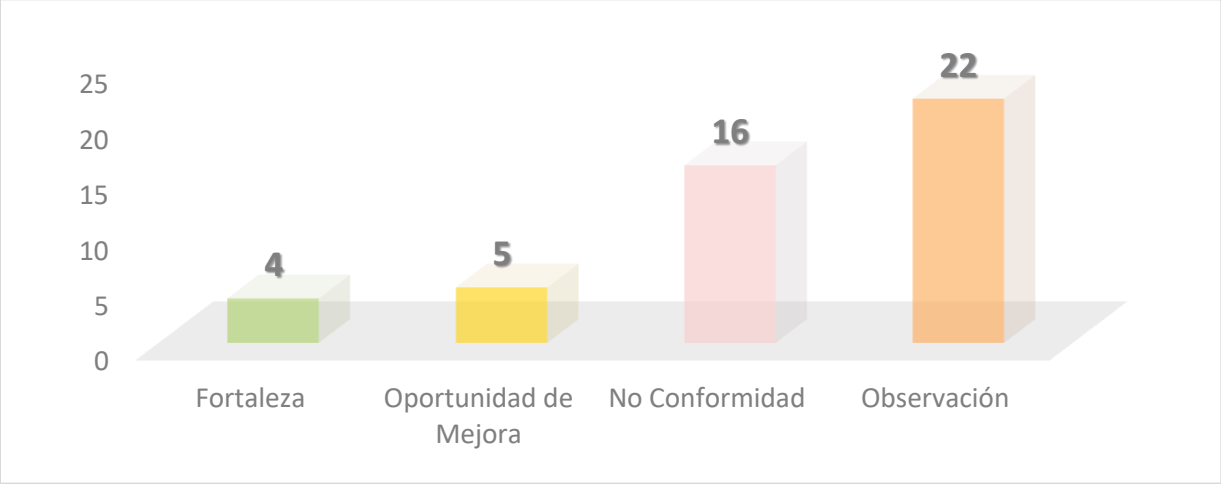
Auditoría de primera parte al Sistema de Gestión de Seguridad de la Información con base en el estándar ISO/IEC 27001:2013 en los 18 procesos de la Autoridad Nacional de Licencias Ambientales (ANLA).

Antes de la Auditoría, ANLA, facilitó su Alcance del SGSI, Políticas y objetivos de seguridad de la información, Declaración de aplicabilidad, Mapa de procesos, inventario de activos de la información, revisión de la dirección y último informe de auditoría interna para que fuesen revisados. Por lo cual se realizó el Análisis del Sistema Documental previo.

Los cinco (5) días de Auditoría se llevó a cabo en las instalaciones de la ANLA Carrera 13A # 34 - 72 en Bogotá D.C y se han mantenido conversaciones con miembros de todos los Procesos. El alcance original de la Auditoría fue revisado y ajustado para que fuese apropiado para las actividades que se están llevando a cabo.

En la reunión de Cierre, la Dirección fue informada de la eficacia del sistema de gestión mediante presentación gerencial, previamente remitida el día 05 de Septiembre de 2023.

A continuación se presenta un resumen de los hallazgos:



3. FORTALEZAS

1. La alta dirección de ANLA dispone recursos económicos, los cuales son detallados en el sistema de información (SPGI) evidenciados en las diversas soluciones tecnológicas adquiridas, desarrolladas e implementadas por la ANLA para el cumplimiento de los objetivos del SGSI.

2. ANLA ha desarrollado de manera In-house a la medida para sistemas de información GESPRO para control y gestor de documentos, Griesgos, Sistema de Planeación y Gestión Institucional (SPGI), con lo cual evitan transferir riesgos y aseguran los controles requeridos.

3. La alta dirección de ANLA dispone recursos económicos, los cuales son detallados en el sistema de información (SPGI) evidenciados en las diversas soluciones tecnológicas adquiridas, desarrolladas e implementadas por la ANLA para el cumplimiento de los objetivos del SGSI.

4. Cuando ocurren no conformidades la ANLA revisa a profundidad la eficacia de las acciones correctivas ejecutadas

4. REQUISITOS CON CUMPLIMIENTO (CONFORMIDADES)

El detalle de la conformidad de los requisitos de los siete (7) cláusulas y de los ciento catorce (114) controles del estándar auditado, se pueden validar en el formato de lista de chequeo auditoría interna, presentado como anexo al presente informe.

Nota: Incluir cuadro cuantas veces sea necesario de acuerdo al cumplimiento de algunos de los criterios establecidos en la auditoria.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
		Detalle del criterio transcrito
DETALLE		

5. DESCRIPCIÓN DE NO CONFORMIDADES

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
1	**6. / 8.2 / 8.3**	**Acciones para tratar riesgos y oportunidades** **Valoración de riesgos de la seguridad de la información** **Tratamiento de riesgos de la seguridad de la información**	**Crítica**
DETALLE DE LA NO CONFORMIDAD			
La actual identificación, análisis, valoración y tratamiento de riesgos tanto del SGSI como de seguridad de la información, no permite asegurar que la ANLA logre los resultados previstos, prevenga y reduzca efectos indeseados sobre el SGSI, toda vez que se ha omitido la aplicación de las fases en mención sobre riesgos específicos, incluso relacionados con amenazas y vulnerabilidades determinadas en la DP-PLE-01 Política de administración de riesgos V7 y entre otras metodologías en la norma ISO 27005:2018 para gestión de activos y seguridad de la información definida por la ANLA como estándar para riesgos de seguridad de la información. Por ejemplo: No se han identificado amenazas como el Cross Site Scripting ni el SQL injection y los controles aplicados en la actualidad son insuficientes para su aseguramiento definitivo, pues mediante la presente auditoría se definieron estado de conformidad como Observación.			
CAUSA: No se siguen las pautas de la norma ISO 27005:2018, incluso esta norma sólo es mencionada pero no detallada en la DP-PLE-01 Política de administración de riesgos V7. Incluso esta norma ya fue actualizada a la versión 2022. Nota: no es necesario aplicar totalmente la norma en mención, sin embargo, es una de las posibles referencias metodológica más adecuadas.			
CONSECUENCIA: No identificar, analizar, valorar, ni tratar riesgos de seguridad de la información, lo cual puede generar que se presenten incidentes por controles aplicables no establecidos, implementados, mantenidos ni mejorados.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
2	**A.11.2.6**	**Seguridad de equipos y activos fuera de las instalaciones**	**Crítica**
DETALLE DE LA NO CONFORMIDAD			
No se cuenta con medidas de seguridad estandarizadas ni aplicadas en los activos de información con alto grado de sensibilidad que se encuentran fuera de las instalaciones de ANLA, como lo son los equipos de cómputo de los contratistas y algunos funcionarios, esto teniendo en cuenta los diferentes riesgos de trabajar fuera de las			

instalaciones. Pese a que recientemente el grupo de seguridad de la información ha requerido a los contratistas que aseguren sus equipos mediante controles de Antivirus, VPN y DLP de la solución adquirida por la ANLA (*Harmony Endpoint*), los equipos tomados como muestra no tienen aplicado estos controles.
CAUSA: Posible falta de efectividad en los mecanismos de divulgación, comunicación, capacitación, seguimiento y/o acompañamiento de parte del Grupo de seguridad a los colaboradores o contratistas con equipos de cómputo propios.
CONSECUENCIA: Existe la posibilidad de que un equipo sea contaminado con malware y que a su vez contamine archivos que luego pueden ser cargados en los sistemas de información de la ANLA.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
3	**A.17.2.1**	**Disponibilidad de instalaciones de procesamiento de información**	**Crítica**
DETALLE DE LA NO CONFORMIDAD			
Pese a contar con Firewall de continuidad físicos y virtuales, en alta disponibilidad y en conectividad, la ANLA no cuenta con instalaciones de procesamiento alternas que permitan la redundancia suficiente para cumplir los requisitos de disponibilidad. Nota: Es importante tener en cuenta que mediante este ejercicio no se auditaba la norma ISO 22301:2019, sin embargo, el estándar ISO/IEC 27001:2013 es claro en sus objetivos de control que requieren asegurar la disponibilidad de instalaciones redundantes de procesamiento de información, sin lo cual no se asegura uno de los tres atributos objeto de la adopción y aplicación del estándar auditado.			
CAUSA: Inadecuada planificación.			
CONSECUENCIA: Si el proveedor del centro de procesamiento de datos principal es atacado o sufre indisponibilidad de los servicios, puede afectar a la ANLA en cuanto a la prestación de los servicios misionales y a sus partes interesadas, por no contar con centro de procesamiento de respaldo con las debidas medidas de protección.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
4	**A.6.1.2**	**Separación de deberes**	**-**
DETALLE DE LA NO CONFORMIDAD			
El Jefe de la Oficina de T.I. es el Jefe del Profesional especializado CISO responsable del SGSI.			
CAUSA: Inadecuada planificación.			
CONSECUENCIA: Posibles conflictos de interés entre los cargos en mención, afectando la efectividad del SGSI.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
5	**9.3.**	**Revisión por la dirección**	**-**
DETALLE DE LA NO CONFORMIDAD			

La revisión por la dirección No incluye consideraciones sobre:

- Los cambios en las cuestiones externas e internas que sean pertinentes al SGSI.
  - La retroalimentación sobre el **desempeño de la seguridad de la información (2)**, incluidas las tendencias relativas a: no conformidades y acciones correctivas. **d) Resultado de la Auditoría (no lo están pidiendo)**
- La retroalimentación de las partes interesadas como comunidades y usuarios (que requieren servicios de licencias), *no está incluida en el informe de revisión de la dirección vigente Acta no. 004 de 2023 del 15 de Mayo de 2023* ***d)*** *1, 2 y 3 y el* ***e)***
- Resultados de la valoración de riesgos del SGSI y de la seguridad de la información. *(Pese a lo revisado en Comité coordinación institucional de control interno Acta 31 del 08-11-2022).* ***F)***

CAUSA:
Es posible que al presentarse el informe de revisión de la dirección del SGSI de manera integrada con las otros (3) sistemas de gestión de la ANLA, no se aseguren o validen en detalle todas las entradas requeridas para el SGSI en específico.

CONSECUENCIA:
Ausencia de información de alto valor para la alta dirección, con posibles afectaciones en la efectividad de las decisiones relativas al SGSI.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
6	6.2	**Objetivos de Seguridad de la Información y planes para lograrlos**	-

DETALLE DE LA NO CONFORMIDAD

No es factible medir la efectividad del SGSI respecto al cumplimiento de los objetivos de la política de seguridad de la información.
Lo anterior, pese a que la ANLA ha definido nueve (9) objetivos de seguridad de la información en la Política (estructurada) general de privacidad y seguridad de la información V5 del 12-24-2023, la estructuración y diseño de indicadores y métricas no están directamente relacionadas con los objetivos del SGSI.

CAUSA:
Falta de integración de los Objetivos de seguridad de la información aprobados en la Política (estructurada) general de privacidad y seguridad de la información V5 del 12-24-2023 con las métricas del PETI y los demás KPIs. No se utiliza la actual información con la que cuenta la ANLA para medir la eficacia del SGSI con relación a los objetivos aprobados y comunicados.

CONSECUENCIA:
Ausencia de información de alto valor para la alta dirección relativa a los resultados del SGSI, con posibles afectaciones en la efectividad de las decisiones relativas al SGSI.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
7	4.2	**Comprensión de las necesidades y expectativas de las partes interesadas.**	-

DETALLE DE LA NO CONFORMIDAD

ANLA no determina Grupos de interés tales como la comunidad, la Alta dirección, ni usuarios que requieren servicios de licencias.

CAUSA: La planificación del SGSI no incluye todas partes interesada bien sea cualquier persona u organización que pueda crear, acceder, procesar, suministrar, almacenar, modificar o eliminar activos de la información de o para la ANLA y que por ende dicha parte interesada pueda afectar, verse afectada o percibirse como afectada por una decisión o actividad del SGSI de la ANLA.
CONSECUENCIA: No identificar, analizar, valorar, ni tratar riesgos de seguridad de la información, lo cual puede generar que se presenten incidentes por controles aplicables no establecidos, implementados, mantenidos ni mejorados.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
8	**A.8.2.1**	**Clasificación de la información.**	**-**
DETALLE DE LA NO CONFORMIDAD			
Toda información de tipo pre-concepto o concepto técnico (documentos en construcción), que se clasifican como activos de alto valor para la ANLA no están identificados ni clasificados en el inventario de activos de la información.			
CAUSA: No se integra la gestión de activos de información con la gestión de riesgos de seguridad de la información. No se siguen las pautas de la norma ISO 27005:2018, incluso esta norma sólo es mencionada pero no detallada en la DP-PLE-01 Política de administración de riesgos V7. Nota: no es necesario aplicar totalmente la norma en mención, sin embargo, es una de las posibles referencias metodológica más adecuadas.			
CONSECUENCIA: No identificar, analizar, valorar, ni tratar riesgos de seguridad de la información, en específico en este tipo de activos de información no clasificados puede generar que se presenten incidentes por controles aplicables no establecidos, implementados, mantenidos ni mejorados.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
9	**A.8.2.2**	Etiquetado de la información	**-**
DETALLE DE LA NO CONFORMIDAD			
Algunos documentos como el *Informe de seguridad de la información respecto al uso de cuentas de usuario,* es etiquetado mediante marca de agua como CONFIDENCIAL, no obstante, esta clasificación no corresponde con las definidas en el Manual de clasificación y etiquetado de información V2 25-08-2022.			
CAUSA: No se integra la gestión de activos de información con la gestión de riesgos de seguridad de la información. No se siguen las pautas de la norma ISO 27005:2018, incluso esta norma sólo es mencionada pero no detallada en la DP-PLE-01 Política de administración de riesgos V7. Nota: no es necesario aplicar totalmente la norma en mención, sin embargo, es una de las posibles referencias metodológica más adecuadas.			
CONSECUENCIA:			

Si existe la posibilidad de que los activos de información no sean clasificados, o se clasifiquen de una manera no estandarizada, ANLA no podrá aplicar controles eficaces sobre los activos de información según su clasificación e importancia y por lo tanto, no identificar, analizar, valorar, ni tratar riesgos de seguridad de la información, en específico en este tipo de activos de información no clasificados, lo cual puede generar que se presenten incidentes por controles aplicables no establecidos, implementados, mantenidos ni mejorados.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
10	**A.9.2.6**	**Retiro o ajustes de los derechos de acceso**	**-**
DETALLE DE LA NO CONFORMIDAD			
No se retiran los derechos de acceso a la información de todos los empleados y de usuarios externos al término de su empleo, contrato o acuerdo, pues gestión contractual abre caso 3003 del 26-07-2023 para solicitar retiro de Ángela Cristina Parra quien se había desvinculado formalmente 13 días antes, es decir, el día 13-Julio-2023.			
CAUSA: Posible de falta de toma de consciencia sobre los riesgos que la no conformidad representa. Ausencia de Políticas claras. Baja efectividad en los controles y actividades de monitoreo de altas y bajas de usuarios			
CONSECUENCIA: Una persona recientemente desvinculada de la ANLA puede aprovecharse deliberada y malintencionadamente de los accesos y recursos no deshabilitados al término de su relación contractual y cometer un incidente.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
11	**A.9.4.5**	**Control de acceso a códigos fuente de programas**	**-**
DETALLE DE LA NO CONFORMIDAD			
Los accesos a códigos fuente de programas no se controlan de forma estructurada ni planificada.			
CAUSA Baja estandarización de los procesos. Posible desconocimiento de los riesgos del presente hallazgo. Posibles fallas en la segregación de funciones.			
CONSECUENCIA Posibles pérdidas de la confidencialidad, integridad y/o disponibilidad de un activo de alto valor para la ANLA como lo son las aplicaciones y soluciones de software se desarrollan in-house.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
12	**A.11.2.9**	**Política de escritorio limpio y pantalla limpia**	**-**
DETALLE DE LA NO CONFORMIDAD			
Se almacenan documentos que se representan activos de alto valor y criticidad para la ANLA en el escritorios y repositorios locales de equipos portátiles propios de los funcionarios y de los contratistas.			
CAUSA:			

Posible falta de efectividad en los procesos de toma de consciencia de la política de escritorio limpio y pantalla limpia.
CONSECUENCIA Posibles incidentes por acceso no autorizado a información clasificada o sensible.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
13	**A.16.1.4** **A.16.1.5**	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos.** **Respuesta a incidentes de seguridad de la información.**	**-**
DETALLE DE LA NO CONFORMIDAD			
ANLA aplica lo establecido en el Procedimiento de gestión de incidentes de seguridad de la información V1, sin embargo, no están establecidos ni aplicados procedimientos específicos de respuesta a incidentes basados en escenarios necesarios que debe ser incluso probados por la ANLA.			
CAUSA: Insuficiente planificación y documentación del control.			
CONSECUENCIA: En caso de presentarse cualquier tipo de incidente de seguridad de la información, la ANLA no está preparada para responder mediante procedimientos y actividades estandarizadas ni probadas en términos de contención, erradicación, recuperación y toma de decisiones de manera clara y efectiva. Nota: se reitera, para gran variedad de posibles escenarios aplicables específicos.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
14	**A.17.1.1**	**Planificación de la continuidad de la seguridad de la información**	**-**
DETALLE DE LA NO CONFORMIDAD			
Actualmente se cuenta con Documento en construcción del Plan de continuidad del negocio, el cual incluye escenarios de eventos de interrupción tecnológicos y no tecnológicos, sin embargo, se reitera que no está aprobado. Este documento contiene algunos escenarios para interrupciones tecnológicas y de los procesos del negocio, sin embargo, ninguno contempla el aseguramiento de la seguridad de la información durante la interrupción.			
CAUSA: Insuficiente planificación y documentación del control. Baja estandarización de los procesos.			
CONSECUENCIA: En caso de presentarse cualquier tipo de indisponibilidad de los activos de información o incidente de seguridad de la información, la ANLA no ha probado los niveles de seguridad de la información en situaciones que impliquen la aplicación de estrategias, soluciones y/o planes de continuidad del negocio para gran variedad de posibles escenarios aplicables específicos, incluso adicionales o diferentes a la recuperación de recursos tecnológicos (DRP).			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
15	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	-
DETALLE DE LA NO CONFORMIDAD			
El normograma no incluye legislación ni normas relativas al Teletrabajo (Ley 1221 del 2008 de teletrabajo y Decreto 1227 de 2022), ocurre igual con leyes concernientes a Propiedad intelectual y Derechos de autor.			
CAUSA: Baja efectividad en los controles y actividades de actualización y aseguramiento del normograma en términos puntuales de los requisitos de la ISO/IEC 27001:2013.			
CONSECUENCIA: Posibles incumplimientos de requisitos legales o normativos relativos a la gestión de la seguridad de la información.			

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
16	A.13.2.2	Acuerdos sobre transferencia de información	-
DETALLE DE LA NO CONFORMIDAD			
No se aplican acuerdos de transferencia segura de información del negocio entre la organización y las partes externas relacionados con los procesos de ANLA en específico en los medios de almacenamiento recibidos de parte de los usuarios por parte de Gestión documental.			
CAUSA: Insuficiente planificación y documentación del control. Baja estandarización de los procesos.			
CONSECUENCIA: Posibles incidentes por ausencia de controles y medidas de protección específicas para información clasificada o sensible que se comunica, comparte, trasfiere o trasmite con partes externas de la ANLA.			

6. NO CONFORMIDADES RECURRENTES

No aplica, incluso puesto que no es del todo factible reportar No conformidades recurrentes, teniendo en cuenta que en el informe de Auditoría interna realizada por el ingeniero Raúl Trujillo el 27/10/2022 a seis (6) de los dieciocho (18) procesos de la ANLA, no se reportaron hallazgos de No Conformidad

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD
DETALLE DE LA NO CONFORMIDAD			
CAUSA			
CONSECUENCIA			

NOTA: Dada la recurrencia de la no conformidad, es necesario que el proceso auditado revise la efectividad de las acciones definidas en el plan de mejoramiento (si aplica) para evaluar la pertinencia de su reformulación

7. EVALUACIÓN RIESGOS (Se evalúa en Gesriesgos)

ANLA ha implementado tres (3) Hojas de vidas de riesgos:

RC-CI-12: Posibilidad de eliminación, modificación u ocultamiento de la información que reposa en la plataforma tecnológica de la entidad para beneficio propio o favorecer a un tercero.

RS-CI-56: Posibilidad de indisponibilidad de los sistemas informáticos /o información contenida en estos.

RS-CI-170: Posibilidad de pérdida de confidencialidad e integridad de la información en los sistemas de información de la entidad.

Adicionalmente, el Oficial de seguridad de la información ha facilitado una Matriz de riesgos no oficial del SGSI con un avance hasta valor de riesgo inherente y controles propuestos.

Pese a lo anterior, el hecho de presentar los diferentes hallazgos de la presente auditoría se ha reportado la No conformidad #1 de tipo crítica.

8. OTROS ASPECTOS EVALUADOS (si aplica)

- Autocontrol: *No aplica.*
- Indicadores: *Se reporta el hallazgo de No conformidad #6.*
- Recomendaciones auditoría anterior: *El presente informe explica el enfoque que deben tener las próximas auditorías internas a realizar al SGSI, con base en el estándar internacional ISO/IEC 27001:2013*
- Monitoreo del cambio: *No aplica*
- Conflictos de Interés: *Se reporta el hallazgo de No conformidad #4.*
- Evaluación de Efectividades: *Se reporta el hallazgo de No conformidad #6.*
- Evaluación de las Políticas MIPG: *Revisión realizada al revisar los requisitos cláusulas 5. y Dominio A.5., del estándar internacional ISO/IEC 27001:2013.*

9. OBSERVACIONES (si aplica)

1. Considerar de manera más amplia las interfaces y dependencias de la organización con el objeto de Asegurar el Alcance del SGSI con toda parte interesada o activo soporte aplicable al mismo. **Requisito 4.3. c)**

2. Robustecer el SGSI aplicando eficazmente las acciones correctivas del presente ejercicio de auditoría, con el fin de culminar y afinar su establecimiento, implementación, mantenimiento y mejora continua.
   Requisito 4.4. c)

3. Fortalecer los procesos o medios para hacer disponible la Política de seguridad de la información de ANLA a todas las partes interesadas (internas y externas) que se definan como apropiadas.
   Requisito 5.2. g)

4. Asegurar y fortalecer los procesos o medios para hacer partícipes a los contratistas y empleados de Seguridad Nápoles Ltda., en las actividades de educación, formación y toma de conciencia apropiada, así mismo, en las actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. Adicionalmente, con base en las entrevistas realizadas a los colaboradores de los distintos procesos, no todos son del todo conscientes, incluso, algunos son en cierto grado renuentes a los procesos de toma de consciencia, por lo cual, es importante que ANLA asegure los procesos de toma de conciencia aplicables.
   Nota: Estas entrevistas se realizaron en compañía de Raúl Trujillo, Nohora Velázquez y Liliana Patiño.
   Requisito 7.3.

5. Asegurar y hacer explicita la denominación de la documentación cumpla con los estándares documentales de la norma ISO/IEC 27001:2013, dado que no ha sido óptima la verificación de documentos como políticas y reglamentos dado la simplificación documental.
   Requisito 7.5.

6. Profundizar y asegurar el análisis de causas de las acciones correctivas.
   Requisito 10.1. b2)

7. Asegurar la evaluación de necesidades de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir.
   Requisito 10.1. b3)

8. Para los empleados funcionarios de ANLA que no pertenecen a la OTI, no se encuentra evidencia de acuerdos contractuales con responsabilidades en torno a la seguridad de la información, independiente del tipo de contrato y de los compromisos con la Integridad, transparencia y lucha contra la corrupción de la Función pública.
   Control A.7.1.2

9. Teniendo en cuenta que actualmente se describen y comunican consecuencias relativas a Fugas de información, es preciso para la ANLA asegurar y hacer explícitas las acciones a emprender contra empleados que hayan cometido una violación a la seguridad de la información, frente a

incidentes contra la pérdida de confidencialidad, integridad, disponibilidad, autenticidad y no repudio, incluso, determinando la tipificación y mecanismos basado en un catálogo más amplio de incidentes que complementen el actualmente definido (Fuga de información). Lo anterior, basado en entrevistas con Constanza, María Paula y Sara de Procesos disciplinarios.
Control A.7.2.3

10. Complementar y fortalecer el acceso seguro con el fin de proteger los activos de seguridad con mayor nivel de importancia y clasificación cuenten con los mejores controles disponibles a fin de evitar accesos no autorizados, malintencionados o no, sobre este tipo de información en sistemas de información y servicios que pasan sobre redes públicas, incluso asegurando que los usuarios no guarden contraseñas en el navegador.
Control A.9.2.4

11. Consolidar las políticas de criptografía, pues las directrices están se encuentran en varios documentos tales como: Manuales, Instructivos y lineamientos, etc. Ver (Manual operativo del SGSI, instructivos instructivo de cifrado e integridad de la información, lineamientos de desarrollo seguro. Y profundizar en la especificad de las directrices de estándares, protocolos y mínimos criptográficos, esto dado que, en el título 7 del título 5.9 se definen requisitos de cifrado fuerte pero no se especifican mínimos.
Control A.10.1.1

12. Asegurar los procesos de retiro de activos de las instalaciones de ANLA. Lo anterior, dado que la empresa de Seguridad Nápoles valida la salida de activos superficialmente.
Control A.11.2.5

13. Proteger adecuadamente la totalidad de equipos de cómputo que puedan representar riesgos de malware, estandarizando soluciones y controles pertinentes.
Control A.12.2.1

14. Establecer, documentar, implementar y aplicar criterios para evaluar y tomar las medidas apropiadas de manera oportuna y enfocada con base en la criticidad de los riesgos y activos en caso de presentarse vulnerabilidades técnicas.
Control A.12.6.1

15. Profundizar en la determinación de estándares de codificación segura, para hacer explícitas las medidas preventivas a aplicar de cara a las Amenazas como el SQL-injection y Cross Site Scripting, entre otras.
Control A.14.2.1

16. Robustecer, planificar y documentar la consolidación de las actividades de endurecimiento (Hardening).**Control A.14.2.4**

17. Robustecer la definición formal de los Principios de construcción de los sistemas seguros, asociados con el procedimiento de viabilidad de proyectos de desarrollo de software V3.
Control A.14.2.5

18. ANLA realiza pruebas con datos reales, sin embargo, no aplica técnicas de protección como ofuscamiento, enmascaramiento, etc., este hallazgo lo deben analizar y atender desde la gestión de riesgos y clasificación de los activos de información primaria que se utilicen para dichas pruebas.
Control A.14.3.1

19. Robustecer el Manual de operación del SGSI en el cual se ha establecido en el capítulo 6.1.12 Seguridad para proveedores, a fin de asegurar los controles de seguimiento, revisión y auditoría con regularidad en la prestación de servicios de los proveedores críticos.
Control A.15.1.1

20. Aplicar acuerdos y requisitos de seguridad de la información acordes a la clasificación de los proveedores con base en: los niveles de acceso, procesamiento, almacenamiento y/o comunicación de información crítica o sensible, con el fin de asegurar la aplicación de controles acordes con esta criticidad, así mismo, robustecer y asegurar los controles de auditoría con regularidad en la prestación de servicios de los proveedores críticos independiente del proceso de ANLA que los lidere.
Controles A.15.1.3 y A.15.2.1

21. Asegurar la socialización de conceptos a los funcionarios, y partes interesadas para que no solamente reporten eventos o incidentes, sino también debilidades, brechas, amenazas, etc. relacionadas a la seguridad de la información observada o sospechada en los sistemas o servicios.
Control A.16.1.3

22. Especificar de manera más detallada los procedimientos de identificación, recolección, adquisición y preservación de información que pueda servir como evidencia ante la ocurrencia de un incidente, inclusive es preciso que ANLA fortalezca los procesos de investigación forense post-incidentes.
Control A.16.1.7

Oportunidades de mejora

1. Especificar con mayor detalle las necesidades y expectativas de las partes interesadas.
2. Incluir las exclusiones en todo documento donde describan el Alcance del SGSI. Exclusión: A.14.2.7 Desarrollo externalizado.

3. Robustecer la cláusula 9. de propiedad intelectual del Acuerdo vigente de confidencialidad, el cual aplica actualmente únicamente para funcionarios y contratistas de la OTI.
4. Justificar con mayor profundidad desde el marco legal colombiano la vigencia de las cláusulas de confidencialidad después de la terminación o cambio de empleo, lo anterior, con base en lo explicado por el Dr. Daniel Tarquino.
5. Consolidar las lecciones aprendidas para que estén disponibles a quienes lo requieran.

10. CONCLUSIONES

- La Auditoría interna al Sistema de Gestión de Seguridad de la Información (SGSI) de la Autoridad Nacional de Licencias Ambientales (ANLA) fue realizada sobre la totalidad de procesos, con base en el alcance previamente confirmado e incluyendo la totalidad de cláusulas y controles aplicables del estándar internacional ISO/IEC 27001:2013. (Ver Mapa de procesos).

- La auditoría interna fue llevada a cabo con un enfoque claro y profundo en las interfaces y dependencias de los activos de información sensibles y críticos, de alto valor e importancia en el marco de los objetivos estratégicos de la ANLA.

- En términos generales y a pesar de los esfuerzos, inversiones e incluso de la óptima implementación de algunas soluciones tecnológicas de última tecnología, la ANLA no ha culminado la implementación, mantenimiento y mejora continua del SGSI, dados los tres (3) hallazgos de No conformidad críticos reportados y los hallazgos de no conformidad con consecutivo (5 y 6), relativos a la evaluación del sistema, teniendo en cuenta la ausencia de algunas entradas de revisión de la dirección y la estructuración y diseño de indicadores y métricas, puesto que no están directamente relacionadas con los objetivos del SGSI.

11. RECOMENDACIONES

- No se recomienda que la ANLA se presente al proceso de Auditoría para otorgamiento de certificación del SGSI con base en ISO/IEC 27001:2013 principalmente a causa de tres (3) No conformidades críticas que se presentan actualmente.

- Se recomienda que la ANLA de cierre completo y eficaz a la totalidad de hallazgos de No conformidad y Observaciones reportadas antes de presentarse al proceso de Auditoría para otorgamiento de certificación.

- Es importante que la ANLA evalúe, complemente e integre su actual y cabal cumplimiento, con relación a la legislación y normatividad aplicable al sector público, con los requisitos del estándar internacional ISO/IEC 27001:2013.

FIRMA JEFE DE CONTROL INTERNO Y/O AUDITOR LIDER